

# **Signature and Handwriting Activities and Perspectives**



**ATVS – Biometric Recognition Group**  
**Universidad Autónoma de Madrid, Spain**

**Fernando Alonso-Fernandez**

on behalf of

**Julian Fierrez, Manuel Freire, Marcos Martinez-Diaz,**  
**Javier Galbally and Javier Ortega-Garcia**



COST 2101 Action - Workshop on Signature and Handwriting Analysis for Person Identification



- 1. ATVS – Biometric Recognition Group**
- 2. Biometric databases**
- 3. Online signature**
  - Verification systems
  - Handheld devices
  - Vulnerabilities
  - Template protection
- 4. Offline signature**
- 5. Handwriting recognition**
- 6. Challenges**

## 1. ATVS – Biometric Recognition Group

### 2. Biometric databases

### 3. Online signature

- Verification systems
- Handheld devices
- Vulnerabilities
- Template protection

### 4. Offline signature

### 5. Handwriting recognition

### 6. Challenges

## 1. ATVS – Biometric Recognition Group

### STAFF

- 1 Full Professor
- 3 Associate Professor
- 1 Postdoc researcher under a Marie Curie Fellowship
- 5 PhD awarded with official Spanish grants



### PUBLICATIONS (since 2002)

- 20 International JCR Journal Articles
- 15 Springer LNCS
- 4 Book chapters
- >50 International Refereed Conference Papers

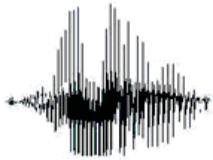


### ORGANIZATION OF INTERNATIONAL EVENTS: FVC 2006, Odyssey 2004

### SEVERAL PUBLIC NATIONAL AND INTERNATIONAL PROJECTS

# 1. ATVS – Biometric Recognition Group

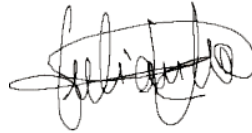
## FIELDS OF EXPERTISE



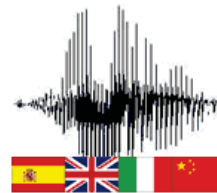
**Speech**



**Fingerprint**



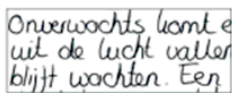
**Signature**



**Language  
recognition**



**Iris**



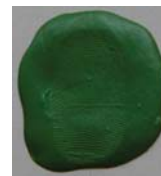
**Handwritting  
g**



**Multibiometric  
s**



**Forensic  
Biometric**



**Vulnerabilitie  
s**



**Databases**

## 1. ATVS – Biometric Recognition Group

## 2. Biometric databases

## 3. Online signature

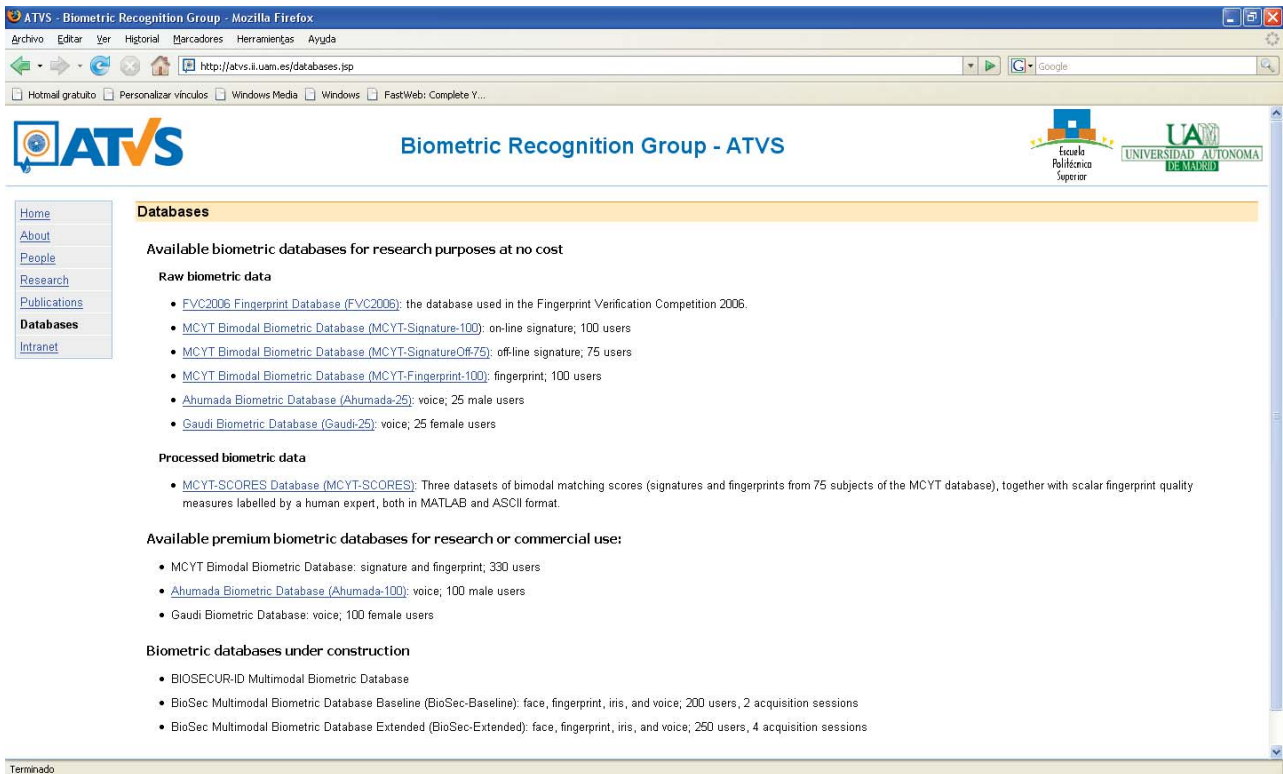
- Verification systems
- Handheld devices
- Vulnerabilities
- Template protection

## 4. Offline signature

## 5. Handwritting recognition

## 6. Challenges

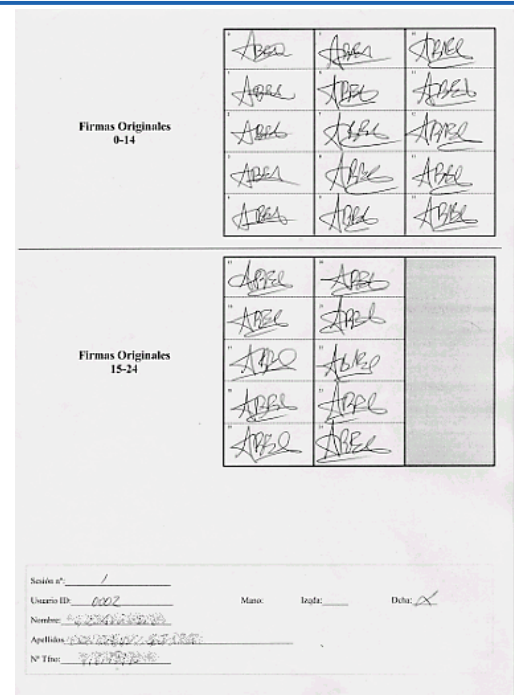
## 2. Biometric databases



## 2. Biometric databases

### MCYT BIMODAL DATABASE

- **330** individuals acquired in 4 Spanish institutions
- Fingerprint and signature data, **1 session**
- Fingerprint: optical and capacitive sensor
- Signature: digitizing Tablet WACOM Intuos
- For each individual: **25 genuine signatures + 25 skilled forgeries**
- **Offline data** from 75 individuals also available



J. Ortega-Garcia, *et al.*, "MCYT Baseline Corpus: a Bimodal Biometric Database", IEE Proc. Vision, Image and Signal Processing, Vol. 150, No. 6, pp. 391-401, 2003.

## 2. Biometric databases

### BIOSECUR-ID MULTIMODAL DATABASE

- **400** individuals acquired in 7 Spanish institutions
- **8 Modalities:** speech, iris, face, **signature and handwriting (on-line and off-line)**, fingerprints, hand and keystroking.
- **4 Sessions.** Three levels of temporal variability:
  - Within the same session.
  - Within weeks (consecutive sessions).
  - Within months (non consecutive sessions)



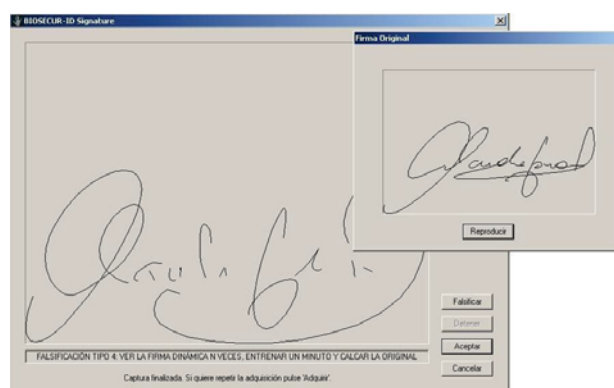
J. Galbally, J. Fierrez, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez et al., "BiosecurID: a Multimodal Biometric Database", in Proc. MADRINET Workshop, Salamanca, Spain, November 2007 (to appear).

## 2. Biometric databases

### BIOSECUR-ID MULTIMODAL DATABASE

#### Signature (on-line and off-line):

- 4 genuine signatures
- 1 forgery of each of the precedent three donors. **4 levels of forgery**
  - Session 1: see once and imitate
  - Session 2: see once, train 1 minute and imitate
  - Session 3: see 3 times, train 1 minute and imitate
  - Session 4: see as many times as you want, train 1 minute and imitate



J. Galbally, J. Fierrez, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez et al., "BiosecurID: a Multimodal Biometric Database", in Proc. MADRINET Workshop, Salamanca, Spain, November 2007 (to appear).



## 2. Biometric databases

### BIOSECUR-ID MULTIMODAL DATABASE

#### Handwriting (on-line and off-line):

- Spanish text in lower-case
- The 10 digits written separately
- 16 Spanish separate words in upper-case

a kilómetros le ans hermanos suri vencesho arroy  
 luz: la grafística es el análisis de los documentos  
 dubitados, y probablemente puede decirse que la grafística  
 es la presentata de la ciencia forense ya que no  
 es una disciplina que haya surgido de modo  
 propio, sino que se necesitó desde los orígenes de  
 los sistemas judiciales; apareciendo ya casos desde  
 los días del imperio romano, aunque hasta siglos  
 después no se incorporó en los juicios finalmente.

|                    |               |
|--------------------|---------------|
| BIODEGRADABLE      | ESPRESEIVIDAD |
| DECEENABLE         | INTELENTABLE  |
| DESAPROVECHAMIENTO | INTEZIGNABLE  |
| DESABRIGAR         | INPATISABLE   |
| DESLUMBRAMIENTO    | INGOBERNABLE  |
| DESDEBATEMENTO     | MANSEBUNABLE  |
| DESAPRENDER        | ZAFARRANCHO   |
| ENGUALDRAR         | ZARZIGASTROSA |

1 2 3 4 5 6 7 8 9 0

J. Galbally, J. Fierrez, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez et al., "BiosecurID: a Multimodal Biometric Database", in Proc. MADRINET Workshop, Salamanca, Spain, November 2007 (to appear).

## 2. Biometric databases

### BIOSECURE MULTIMODAL DATABASE

- 11 European institutions
- Three datasets, 2 sessions:
  - DS1 – Internet (>900 individuals): Voice, face
  - DS2 – Desktop (>600 individuals): Voice, face, **signature**, fingerprint, iris, hand
  - DS3 – Mobile indoor/outdoor (>600 individuals): : Voice, face, **signature**, fingerprint

DS2: Controlled quality data  
(x, y, pressure, angles)



DS3: Degraded condition  
(x, y)



## 1. ATVS – Biometric Recognition Group

## 2. Biometric databases

## 3. Online signature

- **Verification systems**
- **Handheld devices**
- **Vulnerabilities**
- **Template protection**

## 4. Offline signature

## 5. Handwriting recognition

## 6. Challenges

J. Fierrez and J. Ortega-Garcia, "On-line signature verification", A. K. Jain, A. Ross and P.Flynn (Eds.), Handbook of Biometrics, 2007 (to appear)

## 3. Online signature verification

### THREE APPROACHES FOR SIGNATURE VERIFICATION

#### FUNCTION-BASED APPROACH USING LOCAL HMM MODELLING:

- Signature is modelled using the **dynamic time sequences (x,y,p,angles)**

J. Fierrez, D. Ramos-Castro, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: feature extraction and signature modeling", Pattern Recognition Letters, Vol. 28, n. 16, pp. 2325-2334, December 2007

#### FUNCTION-BASED APPROACH USING LOCAL DTW MODELLING

- Matching of time functions is done using elastic distance measures (DTW)
- Better than the HMM with **few training data**

J. Fierrez-Aguilar, S. Krawczyk, J. Ortega-Garcia, and A. K. Jain, "Fusion of Local and Regional Approaches for On-Line Signature Verification", Proc. of IWBRs, pp.: 188-196, Springer LNCS-3781, 2005.

#### FEATURE-BASED APPROACH USING GLOBAL PARAMETERS:

- Signature is modelled with a set of **holistic parameters**.
- Advantages: **easy and quick** to compute (e.g. handheld devices)
- Better than the HMM with **few training data**

J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, J. Ortega-Garcia, and D. Maltoni, "An On-Line Signature Verification System Based on Fusion of Local and Global Information", Proc. 5th IAPR Intl. Conf. on Audio- and Video-based Biometric Person Authentication, AVBPA-05, pp. 523-532, July 2005, LNCS-3546.

### 3. Online signature verification

#### SIGNATURE VERIFICATION USING HANDHELD DEVICES

- We are currently developing **systems adapted to handheld devices** via adaptation of previously developed systems.
- Dynamic signature verification can be incorporated in commercial handheld devices and smart-phones.
- **Touch-screens** provide a straightforward means of online signature acquisition.
- Automatic Signature Verification systems on handheld devices must have **low processing and memory requirements**



M. Martinez-Diaz, J. Fierrez, J. Galbally, F. Alonso-Fernandez and J. Ortega-Garcia, "Signature verification on handheld devices", in Proc. MADRINET Workshop, Salamanca, Spain, November 2007 (to appear)

F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Secure access system using signature verification over Tablet PC", IEEE Aerospace and Electronic Systems Magazine, Vol. 22, n. 4, pp. 3-8, April 2007

### 3. Online signature verification

#### APPLICATIONS ON HANDHELD DEVICES

- Main application on handheld devices include:
  - Payments in **commercial environments**, via UMTS, GPRS, WiFi, etc.
  - **Legal transactions**: Legal documents or certificates, E-government applications
  - **User login**: Access control, Local or remote system and networks
  - **Client validation**: E.g. parcel delivery



M. Martinez-Diaz, J. Fierrez, J. Galbally, F. Alonso-Fernandez and J. Ortega-Garcia, "Signature verification on handheld devices", in Proc. MADRINET Workshop, Salamanca, Spain, November 2007 (to appear)

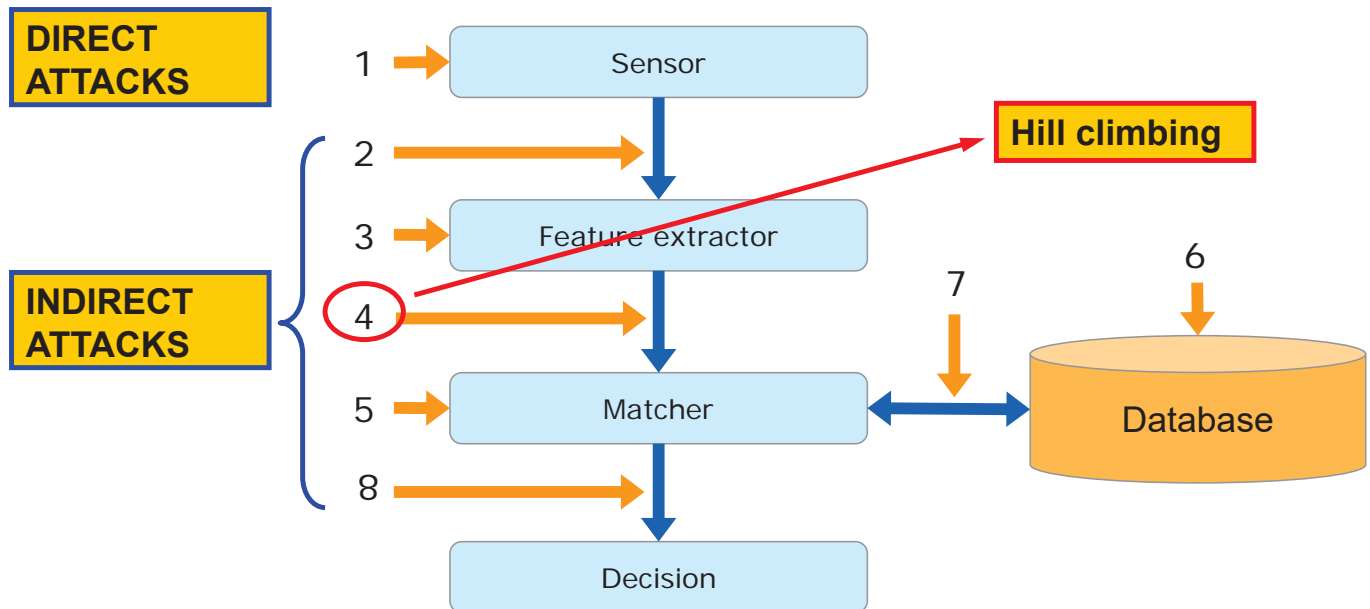
F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Secure access system using signature verification over Tablet PC", IEEE Aerospace and Electronic Systems Magazine, Vol. 22, n. 4, pp. 3-8, April 2007



### 3. Online signature verification

#### VULNERABILITIES OF SIGNATURE VERIFICATION SYSTEMS

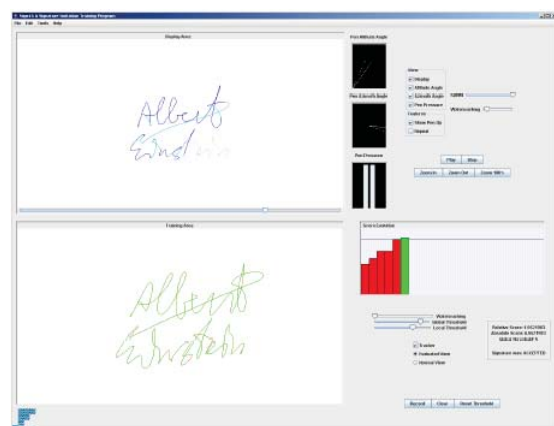
- Biometric systems are not free from external attacks.
- In 2001, Ratha identified and classified 8 possible points of attack



### 3. Online signature verification

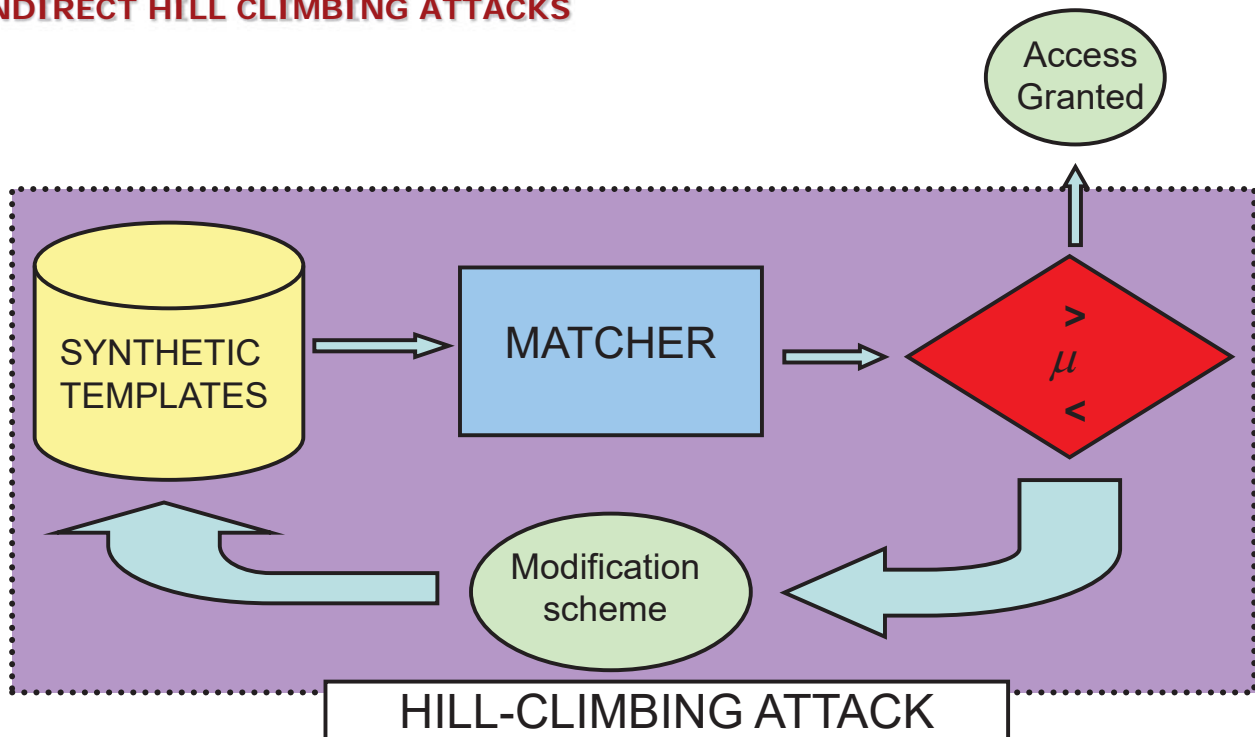
#### DIRECT ATTACKS

- Different levels of forgery:
  - **Random forgery:** a different user signature
  - **Blind forgery:** descriptive information of the signature (ej: name of the user)
  - **Low-force forgery:** visual static information of the signature
  - **Brute-force forgery:** dynamic information of the signature and dedicated tools



### 3. Online signature verification

#### INDIRECT HILL CLIMBING ATTACKS



J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Bayesian hill-climbing attack and its application to signature verification," in Proc. ICB. 2007, pp. 386-395, LNCS-4642.

### 3. Online signature verification

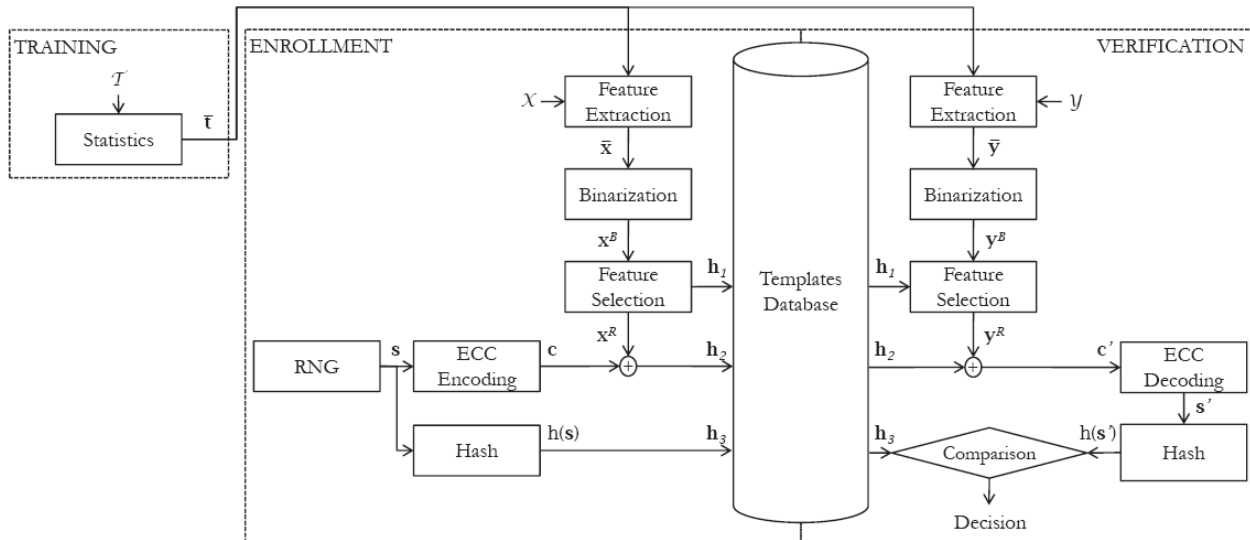
#### TEMPLATE PROTECTION

- With the growth in scale of biometric systems deployed in the last years, **privacy issues** related to the **protection of biometric patterns** have emerged as a crucial challenge for the widespread use of biometrics.
- Template protection systems aim to enhance the **resilience of biometric data against attacks**, while still allowing the matching to be performed efficiently.
- Coarse classification:
  - **Feature transformation:** features are transformed using a one-way function, and matching takes place in the transformed domain
  - **Biometric cryptosystems:** a biometric is used for data encryption/decryption. Template protection is achieved because the biometric is bound to a random binary key.

### 3. Online signature verification

#### TEMPLATE PROTECTION: HELPER DATA SYSTEM

- Feature transformation to binary vectors
- The binary feature vector is combined with a (cancelable) binary random key

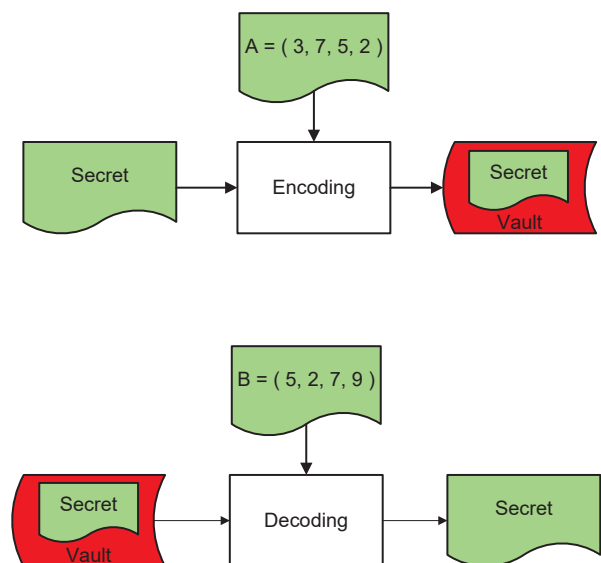


M. R. Freire, J. Fierrez and J. Ortega-Garcia, "Dynamic signature verification with template protection using helper data", Technical Report, Biometric Recognition Group-ATVS, 2007.

### 3. Online signature verification

#### TEMPLATE PROTECTION: FUZZY VAULT

- Alice hides a (cancelable) random key  $S$  in a vault using her enrollment biometric template  $A$
- She will be able to recover the key if she presents a biometric template  $B$  that overlaps substantially with  $A$
- Is a:
  - Biometric cryptosystem: the protected key can be used for cryptography
  - Template protection system: from the vault an attacker cannot recover neither the secret key nor the biometric pattern



M. Freire-Santos, J. Fierrez-Aguilar and J. Ortega-Garcia, "Cryptographic key generation using handwritten signature", in Defense and Security Symposium, Biometric Technologies for Human Identification, BTHI, Proc. SPIE, Vol. 6202, pp. 225-231, Orlando, USA, April 2006

M. R. Freire, J. Fierrez, M. Martinez-Diaz and J. Ortega-Garcia, "On the applicability of off-line signatures to the fuzzy vault construction", in Proc. Intl. Conf. on Document Analysis and Recognition, ICDAR, IEEE Press, Curitiba, Brazil, September 2007.

## 1. ATVS – Biometric Recognition Group

## 2. Biometric databases

## 3. Online signature

- Verification systems
- Handheld devices
- Vulnerabilities
- Template protection

## 4. Offline signature

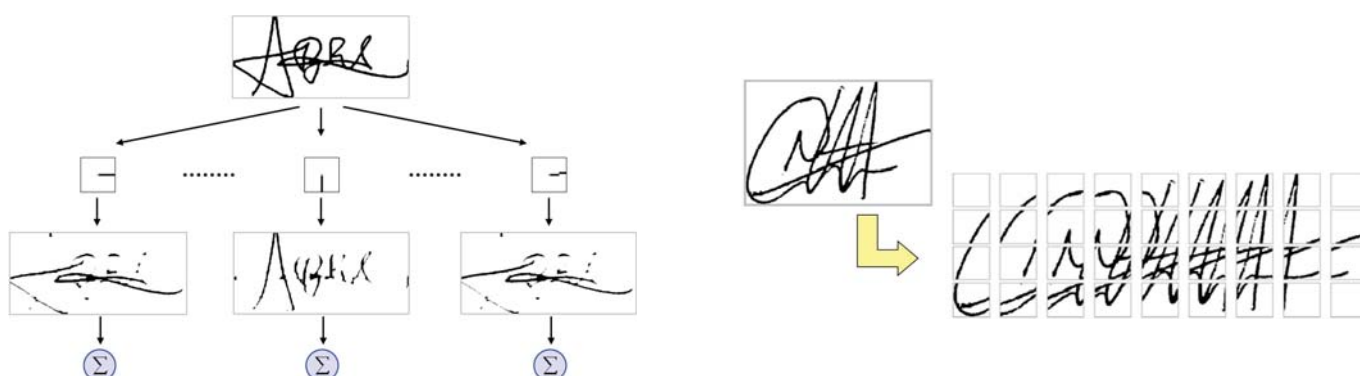
## 5. Handwriting recognition

## 6. Challenges

## 4. Offline signature verification

### TWO APPROACHES FOR SIGNATURE VERIFICATION

- Main applications of offline signature verification: **government, legal and commercial transactions**
- Global image analysis and minimum distance classifier
- Local image analysis and HMM modeling



J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez and J. Ortega-Garcia, "An off-line signature verification system based on fusion of local and global information", in Proc. BIOAW, Springer LNCS-3087, pp. 295-306, Prague, Czech Republic, May 2004

## 4. Offline signature verification

### SIGNAL QUALITY ANALYSIS

- Measures able to **predict the performance** of a verification system



F. Alonso-Fernandez, M. C. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Automatic measures for predicting performance in off-line signature", in IEEE Proc. Intl. Conf. on Image Processing, ICIP, San Antonio TX, USA, September 2007

F. Alonso-Fernandez, M. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Impact of signature legibility and signature type in off-line signature verification", in Biometrics Symposium, BSYM, Baltimore, Maryland (USA), September 2007

### 1. ATVS – Biometric Recognition Group

### 2. Biometric databases

### 3. Online signature

- Verification systems
- Handheld devices
- Vulnerabilities
- Template protection

### 4. Offline signature

### 5. Handwriting recognition

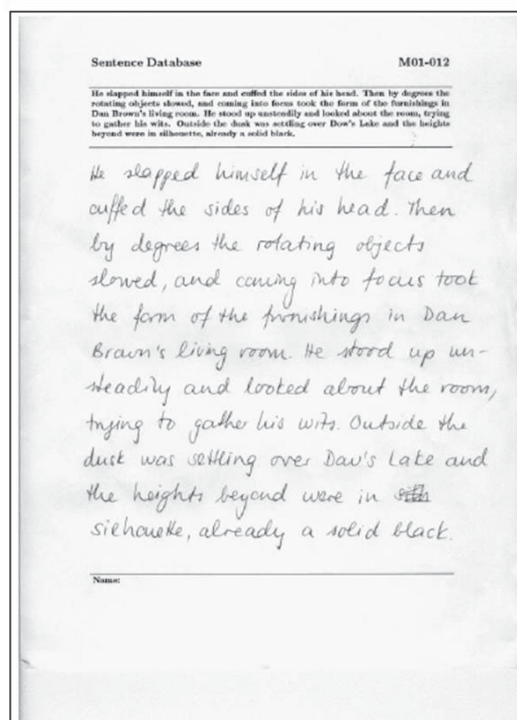
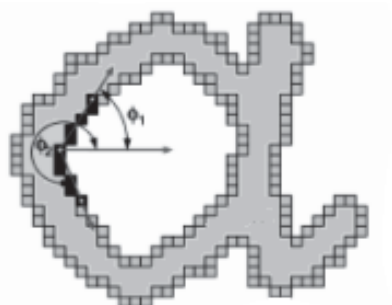
### 6. Challenges



## 5. Offline handwriting recognition

### VERIFICATION SYSTEM BASED ON TEXTURE INFORMATION

- Texture information:
  - Slant orientation, curvature, etc.
  - **Text independent**
- Main applications of offline handwriting recognition: **forensic analysis, historical documents**
- Influence of:
  - **Size of the database** in identification
  - Amount of data



1. ATVS – Biometric Recognition Group
2. Biometric databases
3. Online signature
  - Verification systems
  - Handheld devices
  - Vulnerabilities
  - Template protection
4. Offline signature
5. Handwriting recognition
6. Challenges

## 6. Challenges

### Poor ergonomics and small input areas of handheld devices

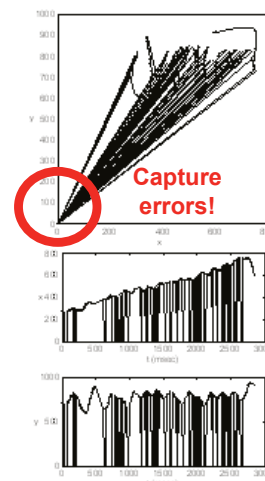
- Increase variability

### Low touch-screen digitizing quality of handheld devices

- Noise
- Missing samples
- No pressure, elevation or pen-azimuth information

### Security

- In case of a security breach an attacker can gain access to financial or legal information of a user.
- Access to the matcher can lead to brute force or hill-climbing attacks among others.
- User template and communications channels must be secured.



## COST 2101 Action Workshop on Signature and Handwriting Analysis for Person Identification

# Signature and Handwriting Activities and Perspectives



## ATVS – Biometric Recognition Group Universidad Autónoma de Madrid, Spain

**Fernando Alonso-Fernandez**

on behalf of

Julian Fierrez, Manuel Freire, Marcos Martinez-Diaz,  
Javier Galbally and Javier Ortega-Garcia